PATENT ABSTRACTS OF JAPAN

(11)Publication number : **06-289782**
(43)Date of publication of application : **18.10.1994**

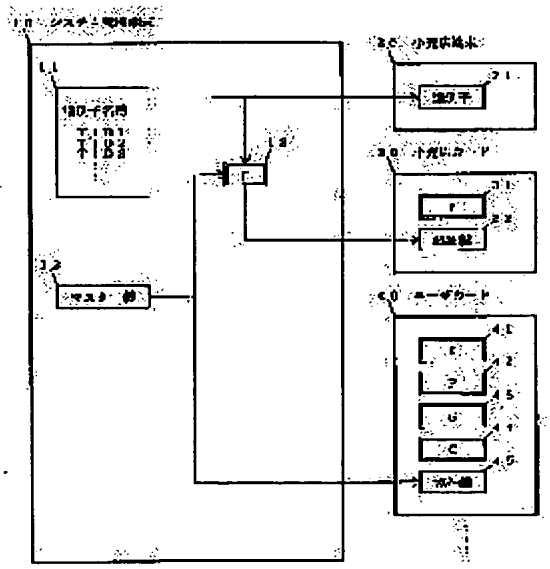
(51)Int.CI. G09C 1/00
G06K 19/073
H04L 9/00
H04L 9/10
H04L 9/12

(21)Application number : **05-080508**
(22)Date of filing : **07.04.1993**

(71)Applicant : **MATSUSHITA ELECTRIC IND CO LTD**
(72)Inventor : **MUTO YOSHIHIRO**
TAKAGI SHINYA

(54) MUTUAL AUTHENTICATION METHOD

(57)Abstract:
PURPOSE: To provide a mutual authentication method with which an IC card system, that necessitates a justification confirmation of an information processing terminal which processes IC cards, is constructed.
CONSTITUTION: The system consists of a system control terminal 10, a retail store terminal 20, a retail store card 30 and user cards 40. An operation means 'f' for an authentication process is beforehand stored in the card 30 and the user cards 40 store the means 'f', a generation means 'F' which generates key data used in the authentication process, a pseudorandom number generating means 'G' and an authentication confrimation means 'C'. The terminal 10 records an authentication, which is unique to the terminal 20, in the terminal 20 and moreover, secret information is recorded in the card 30 and the cards 40.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平６－２８９７８２

(43)公開日　平成６年（１９９４）１０月１８日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
G09C 1/00		8837-5L		
G06K 19/073				
H04L 9/00				
9/10				
9/12				

審査請求　未請求　請求項の数２　ＯＬ　（全８頁）　最終頁に続く

(21)出願番号　特願平５－８０５０８

(22)出願日　平成５年（１９９３）４月７日

(71)出願人　０００００５８２１
松下電器産業株式会社
大阪府門真市大字門真１００６番地

(72)発明者　武藤　義弘
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

(72)発明者　高木　伸哉
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

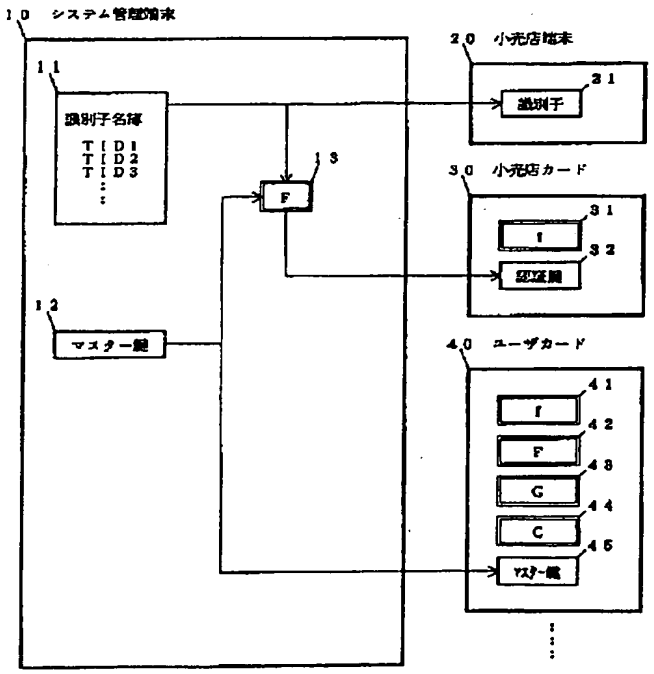
(74)代理人　弁理士　小鍛治　明　（外２名）

(54)【発明の名称】相互認証方法

(57)【要約】

【目的】　ＩＣカードを処理する情報処理端末の正当性確認を必要とするＩＣカードシステムを構築できる相互認証方法を提供する。

【構成】　システム管理端末１０、小売店端末２０、小売店カード３０およびユーザカード４０から成る。予め小売店カード３０には認証処理の演算手段ｆ、また、ユーザカード４０には前記演算手段ｆ、認証処理で使用する鍵データを生成する生成手段Ｆ、疑似乱数生成手段Ｇおよび認証確認手段Ｃが格納されている。システム管理端末１０は、小売店端末２０に端末固有の識別子を記録し、かつ小売店カード３０およびユーザカード４０に秘密情報を記録する。



1

【特許請求の範囲】

【請求項１】固有の識別子を記憶するための第１のメモリ及び暗号化等の処理を行う第１の演算手段及び前記第１の演算手段が演算時に使用する認証鍵を記憶するための第２のメモリを有する情報処理端末と、前記情報処理端末のそれぞれの固有の識別子の名簿を記憶する第３のメモリ及び秘密のマスター鍵を記憶する第４のメモリ及び前記認証鍵を生成する第１の鍵データ生成部を有するシステム管理端末と、前記第１の演算手段と同等の機能を有する第２の演算手段及び前記第１の鍵データ生成部と同等の機能を有する第２の鍵データ生成部及び疑似乱数発生手段及び比較手段及び前記マスター鍵を記憶するための第５のメモリを有する使用者端末とからなるデータ転送システムにおいて、前記システム管理端末は、前記個別の識別子と前記マスター鍵を用いて予め前記第１の鍵データ生成部で認証鍵を作成し、この認証鍵を前記情報処理端末の第２のメモリに格納し、かつ前記システム管理端末は、第２のメモリの記憶している前記マスター鍵を前記使用者端末の第５のメモリの格納しておき、前記情報処理端末と前記使用者端末との間でデータのやりとりが行われる際は、前記情報処理端末の第１のメモリに記憶されている個別の識別子を前記使用者端末が受信し、前記使用者端末の第５のメモリに記憶されている前記マスター鍵を用いて前記第２の鍵データ生成部により認証鍵を作成し、この作成した認証鍵を用いて前記乱数発生手段により発生した乱数を第２の演算手段で演算して前記比較手段に入力し、これと同時並行して前記乱数発生手段より発生した同一の乱数を前記情報処理端末の第１の演算手段に送信し、前記情報処理端末の第１の演算手段は受信した前記乱数を前記第２のメモリに記憶されている認証鍵を用いて演算し、前記比較手段に入力し、前記比較手段は、前記第１の演算手段の出力と前記第２の演算手段の出力とを比較することにより認証処理を行うことを特徴とする相互認証方法。

【請求項２】情報処理端末は第１の演算手段及び第２のメモリを着脱可能な情報担体として配置し、システム使用時に前記情報担体を接続して使用することを特徴とする請求項１記載の相互認証方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】ＩＣカード等を利用したシステムにおける相互認証方法に関する。

【０００２】

【従来の技術】従来の磁気カードを使ったクレジットシステムでは、磁気ストライプの情報、特殊な印刷のフォログラムおよびカードの個人番号によりカードの正当性を、また帳票への署名でカード保有者の正当性確認を行っている。しかし、磁気カードの偽造の容易さ、署名の安全性の低さにより犯罪が多発している。

【０００３】そこで最近では、ＣＰＵ（中央演算装置）とメモリをワンチップで構成し、複製など物理的不正が困難なＩＣカードを利用したシステムが検討あるいはすでに実施されている。

2

【０００４】図４にＩＣカード保有者の確認方式の構成図を示す。ここでは物品を売買する上でのＩＣカード保有者の確認方式について説明する。物を売る側には情報処理端末１００が、物を買う側にはＩＣカード１１０が渡されている。情報処理端末１００には予めサービス提供者（例えばクレジットシステム管理者）によって、疑似乱数生成手段１０１、相手認証のための演算手段１０２、認証確認手段１０３および秘密の鍵データ１０４が格納されている。また、ＩＣカード１１０にも予めサービス提供者によって、情報処理端末１００と同様の演算手段１１３、情報処理端末１００と同様の秘密の鍵データ１１４、パスワード確認手段１１１およびＩＣカード保有者のパスワード１１２が格納されている。

【０００５】物品売買の手続きとして最初に情報処理端末１００は、ＩＣカード１１０に対して疑似乱数生成手段１０１より生成した乱数をＩＣカード１１０に送信すると共に、この乱数に対して秘密の鍵データ１０４と演算手段１０２を用いて演算を施す。一方、ＩＣカード１１０は、情報処理端末１００から受信した乱数に対して秘密の鍵データ１１４と演算手段１１３を用いて演算し、この結果を情報処理端末１００に送信する。情報処理端末１００は、ＩＣカード１１０から受信した結果と先に演算した結果とを認証確認手段１０３により比較し、一致すれば、ＩＣカード１１０には情報処理端末１００と同じ秘密の鍵データ１０４が格納されており正当に発行されたＩＣカードであると判断する。一致しない場合は、不正なＩＣカードと判断し、以降の処理を打ち切る。

【０００６】正当なＩＣカードと判断した場合、次にＩＣカード１１０の保有者の確認を行う。情報処理端末１００は、ＩＣカード保有者から入力されたパスワード（入力方法は情報処理端末１００に付属するキーパッド等から行う。ここでは図示せず）をＩＣカード１１０に送信する。ＩＣカード１１０は情報処理端末１００から受信したパスワードと予め格納されているパスワード１１２とをパスワード確認手段１１１により比較し、この是非の結果を情報処理端末１００に送信する。

【０００７】このように物を売る側は、最初に情報処理端末１００によりＩＣカード１１０の正当性を確認した後、パスワード照合の是非によってカード保有者の確認を行っているため、安全性が高い。すなわちパスワード照合の是非の信頼性が、最初のＩＣカード正当性確認によって得られる。

【０００８】

【発明が解決しようとする課題】従来のシステムでは、店側が一方的にＩＣカードの正当性確認およびＩＣカード保有者の正当性確認を行い、ＩＣカード保有者は店側

を信頼していることを前提にしている。ＩＣカードへのデータの読み書きは、パソコンなどの情報処理端末を通して行っているが、この読み書きは、今後のＩＣカードの多目的利用、すなわち異なった業界のアプリケーションがひとつのＩＣカードに相乗りすることを考慮すると、正当なＩＣカード保有者および正当なサービス提供者の合意のもとに行われなければならない。

【０００９】本発明はかかる点に鑑み、ＩＣカードを処理する情報処理端末の正当性確認を必要とするＩＣカードシステムを構築できる相互認証方法を提供することを目的とする。

【００１０】

【課題を解決するための手段】本発明は上記目的を達成するために、固有の識別子を記憶するための第１のメモリ及び暗号化等の処理を行う第１の演算手段及び前記第１の演算手段が演算時に使用する認証鍵を記憶するための第２のメモリを有する情報処理端末と、前記情報処理端末のそれぞれの固有の識別子の名簿を記憶する第３のメモリ及び秘密のマスター鍵を記憶する第４のメモリ及び前記認証鍵を生成する第１の鍵データ生成部を有するシステム管理端末と、前記第１の演算手段と同等の機能を有する第２の演算手段及び前記第１の鍵データ生成部と同等の機能を有する第２の鍵データ生成部及び疑似乱数発生手段及び比較手段及び前記マスター鍵を記憶するための第５のメモリを有する使用者端末とからなるデータ転送システムにおいて、前記システム管理端末は、前記個別の識別子と前記マスター鍵を用いて予め前記第１の鍵データ生成部で認証鍵を作成し、この認証鍵を前記情報処理端末の第２のメモリに格納し、かつ前記システム管理端末は、第２のメモリの記憶している前記マスター鍵を前記使用者端末の第５のメモリの格納しておき、前記情報処理端末と前記使用者端末との間でデータのやりとりが行われる際は、前記情報処理端末の第１のメモリに記憶されている個別の識別子を前記使用者端末が受信し、前記使用者端末の第５のメモリに記憶されている前記マスター鍵を用いて前記第２の鍵データ生成部により認証鍵を作成し、この作成した認証鍵を用いて前記乱数発生手段により発生した乱数を第２の演算手段で演算して前記比較手段に入力し、これと同時並行して前記乱数発生手段より発生した同一の乱数を前記情報処理端末の第１の演算手段に送信し、前記情報処理端末の第１の演算手段は受信した前記乱数を前記第２のメモリに記憶されている認証鍵を用いて演算し、前記比較手段に入力し、前記比較手段は、前記第１の演算手段の出力と前記第２の演算手段の出力とを比較することにより認証処理を行うことを特徴とする相互認証方法である。

【００１１】また、情報処理端末は第１の演算手段及び第２のメモリを着脱可能な情報担体として配置し、システム使用時に前記情報担体を接続して使用することを特徴とする相互認証方式である。

【００１２】

【作用】この方法により、システム管理者により認められた情報処理端末専用のＩＣカードが無ければ、情報処理端末を通して別のＩＣカード内の情報に対してアクセスすることができないＩＣカードシステムを構築できる。

【００１３】

【実施例】以下、本発明の一実施例について図面を参照しながら説明する。図１は本発明の実施例による鍵データ管理方式を示した構成図である。本実施例では、物品を売買する上でのＩＣカードシステムを考える。２０は小売店端末、３０は小売店カードおよび４０はユーザカードであり、１０はこれら端末、カードおよびＩＣカードシステムを統括的に管理するシステム管理端末である。

【００１４】システム管理端末１０は、認証処理で使用する鍵データを生成する生成手段１３を有しており、システム全体の秘密のマスター鍵をメモリ１２に、かつ、このＩＣカードシステムでの利用を許可した小売店端末の識別子名簿をメモリ１１に記憶している。小売店端末２０は、小売店カード３０と対で使用されるものであり、小売店がシステム管理者より購入あるいは賃貸するものである。小売店カード３０は、予め認証処理の演算手段３１を有している。また、ユーザカード４０は小売店を利用する一般の顧客に配布されるものであり、予め認証処理の演算手段４１、認証処理で使用する鍵データを生成する生成手段４２、疑似乱数生成手段４３、演算手段４１の出力結果と通信相手から受信したデータとを比較する確認手段４４を有している。

【００１５】システム管理端末１０は、小売店に小売店端末２０と小売店カード３０を渡すに際し、小売店端末２０の固有の識別子を小売店端末２０のメモリ２１に格納し、小売店端末２０に固有の識別子とシステム管理端末１０のメモリ１２に格納されているマスター鍵とから生成手段１３により算出した認証鍵を小売店カード３０のメモリ３２に格納する。さらにシステム管理端末１０は、このＩＣカードシステムの加入者に対してユーザカード４０を配布するに際し、システム管理端末１０と同じマスター鍵をユーザカード４０のメモリ４５に格納する。

【００１６】図２は本発明の実施例によるＩＣカードシステムの認証方式を示した構成図である。本発明の鍵データ管理方式により構築されたＩＣカードシステムにおけるユーザカード４０の小売店に対する認証について説明する。なお、物品売買の手続きとして従来の技術で記載している方法でＩＣカードおよびＩＣカード保有者の確認を行う。

【００１７】ユーザカード４０は、小売店端末２０のメモリ２１に格納されている識別子を受信し、メモリ４５に格納されているマスター鍵と生成手段４２を用いて小

5

売店端末２０の秘密の認証鍵を算出し、小売店カード３０との間で共有する。

【００１８】次にユーザカード４０は、小売店端末２０に疑似乱数生成手段４３より生成した乱数を送信すると共に、この乱数に対して先に算出した認証鍵と演算手段４１とを用いて演算を施し、小売店端末２０の認証のために記憶しておく（実際、この処理は小売店端末２０のコマンドにより起動する）。

【００１９】一方小売店端末２０は、ユーザカード４０より受信した乱数を、小売店カード３０に渡す。小売店カード３０は、この乱数に対してメモリ３２に格納されている認証鍵と演算手段３１を用いて演算した結果を小売店端末２０に返し、小売店端末２０はこの演算結果をユーザカード４０に送信する。

【００２０】ユーザカード４０は、小売店端末２０から受信した演算結果と先に記憶していた結果とを認証確認手段４４により比較し、一致すれば、小売店端末２０にはシステム管理端末１０よって正当な秘密の鍵データを格納された小売店カード３０があると判断し、ユーザカード４０内へのデータに対するアクセスを許可し、実際の取り引き処理に移行する。一致しない場合は、不正な小売店と判断しユーザカード４０内へのデータのアクセスを禁止する。なお、小売店カード３０の小売店端末２０に対する認証は、ユーザカード４０と同様な方法であっても良い。

【００２１】本発明の実施例の鍵データ管理方式を用いたＩＣカードシステムでは、小売店端末に第３者が別の小売店カードを挿入してもユーザカードへの不正なアクセスは不可能であり、ユーザカードの安全性を高めることができる。図３は本発明の実施例によるＩＣカードシステムの認証における秘密鍵データ共有方式を示した構成図である。５０および５２は通信相手との間でセッション鍵を共有する第２の生成手段、５１はデータの復号手段、５３はデータの暗号化手段である。

【００２２】小売店カード３０は、ユーザカード４０から受信した乱数に対して演算手段３１により演算を施し、ユーザカード４０に送信した後、この送信したデータとメモリ３２に格納されている認証鍵とから生成手段５０によりセッション鍵を生成する。一方、ユーザカード４０は、確認手段４４の認証結果が正しければ、小売店カード３０と同様に認証鍵と演算手段４１より出力されたデータとから生成手段５２によりセッション鍵を生成し、小売店カード３０との間で共有する。

【００２３】これら共有したセッション鍵を用いて、ユーザカード４０内のデータは暗号化手段５３により暗号化して出力される。小売店端末２０はこの暗号化されたデータを小売店カード３０に渡し、小売店カード３０は復号手段５１により暗号化されたデータの復号を行う。小売店端末２０はこのデータを受け、ユーザカード４０

6

からデータを読みだしたこととなる。

【００２４】この秘密鍵データ共有方式で共有したセッション鍵を用いてユーザカード４０の秘密の固定情報を読み出すと、取り引き毎に毎回異なった暗号文となり、情報の安全性が確保される。またユーザカード４０から小売店カード３０への回線上のデータを第３者が盗聴したとしても、小売店端末２０の専用の小売店カード３０以外のカードでは、この暗号化されたデータは復号できない。なお、ここでは、乱数の暗号化したデータと秘密の認証鍵よりセッション鍵を生成したが、暗号化する前の乱数と秘密の認証鍵よりセッション鍵を生成するようにしても良い。

【００２５】また、本発明の実施例の鍵データ管理方式を用いたＩＣカードシステムでは、小売店の識別子を小売店カードの中に格納し、実際の認証処理においては、小売店端末が小売店カードより小売店の識別子を獲得するようにすることで、小売店カードを有する者はいずれの小売店端末でも利用することができる。ここでは、小売店端末自体に秘密情報を持たす必要がなく、カードの安全な管理のみとなる。

【００２６】なお、上記メリットは無くなり小売店端末の安全な管理が必要となるが、システムコストの低減ということで、小売店カードの機能を小売店端末に持たし、小売店カードを無くすことも可能である。

【００２７】

【発明の効果】以上のように本発明によれば、情報処理端末およびその情報処理装置に対応した正当なＩＣカードが無いと他のＩＣカードへのアクセスが不可能となるＩＣカードシステムを構築できる。

【図面の簡単な説明】

【図１】本発明の実施例による相互認証方法を示した構成図

【図２】本発明の実施例によるＩＣカードシステムの認証方式を示した構成図

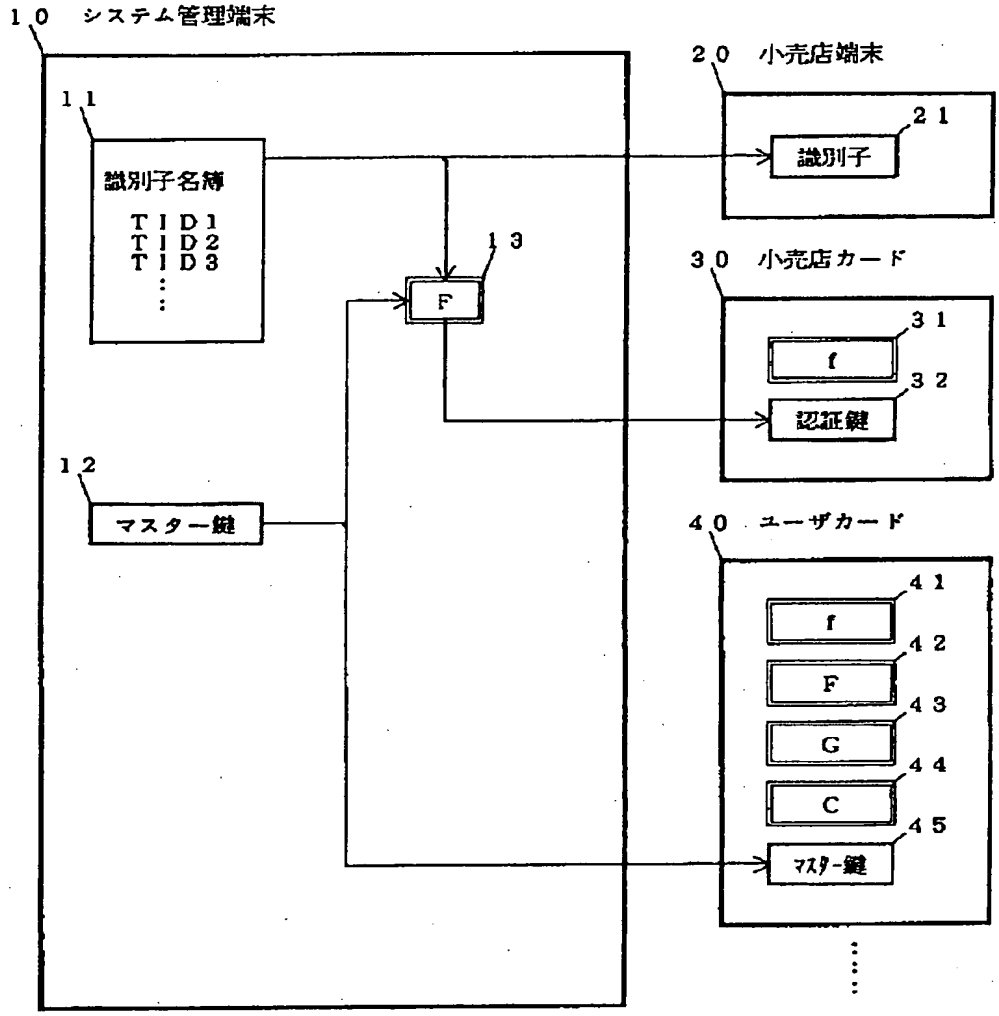
【図３】本発明の実施例によるＩＣカードシステムの認証における秘密鍵データ共有方式を示した構成図

【図４】従来のＩＣカード保有者の確認方式の構成図

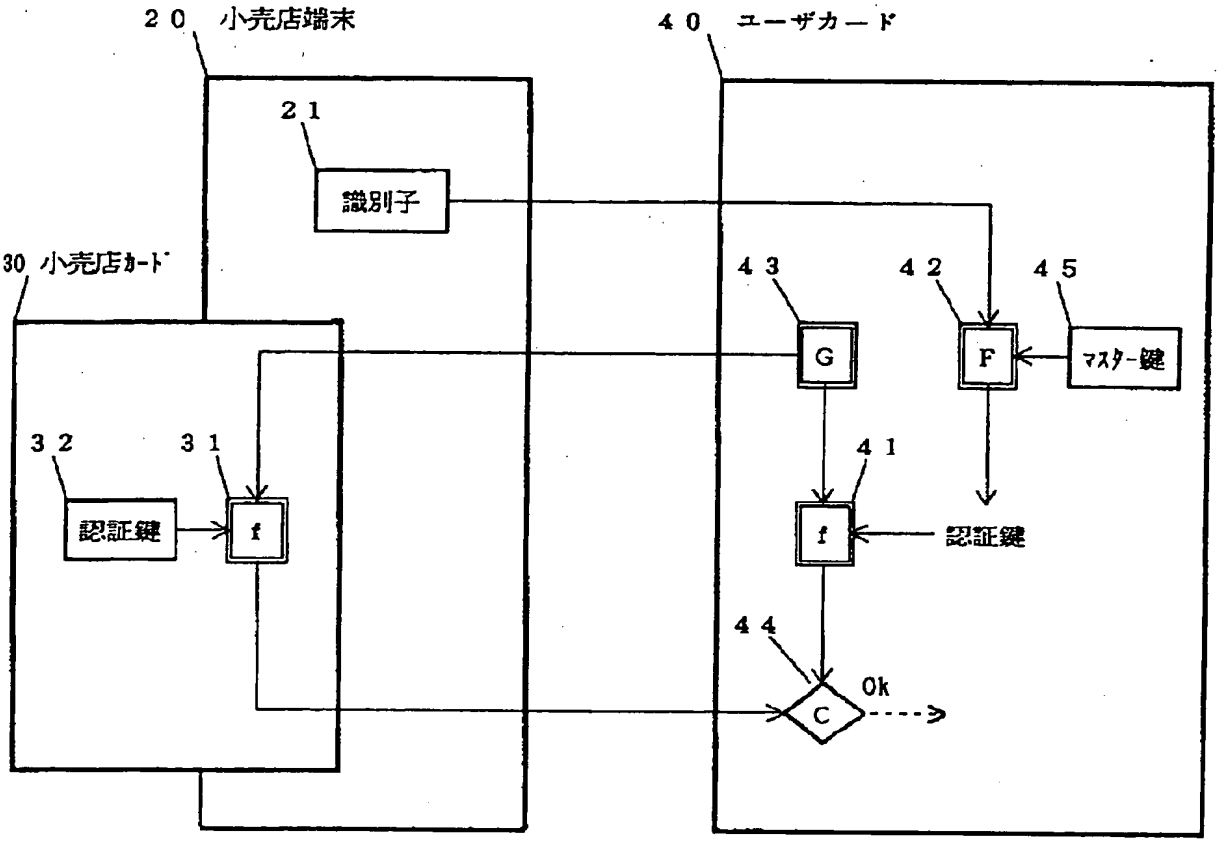
【符号の説明】

１０　システム管理端末
１３　鍵データの生成手段
２０　小売店端末
３０　小売店カード
３１　認証処理の演算手段
４０　ユーザカード
４１　認証処理の演算手段
４２　鍵データの生成手段
４３　疑似乱数生成手段
４４　認証確認手段

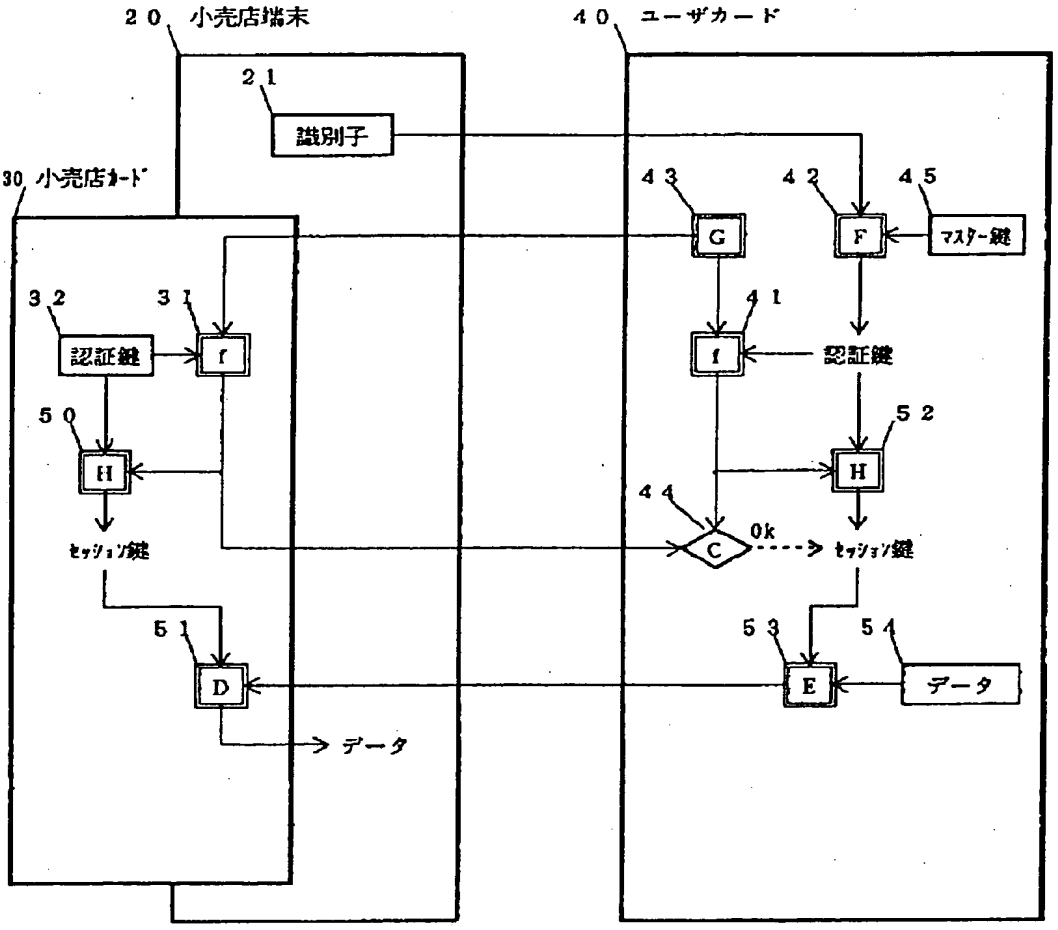
【図１】


１０　システム管理端末
１１
識別子名簿
ＴＩＤ１
ＴＩＤ２
ＴＩＤ３
１２
マスター鍵
１３
F
２０　小売店端末
２１
識別子
３０　小売店カード
３１
f
３２
認証鍵
４０　ユーザカード
４１
f
４２
F
４３
G
４４
C
４５
ﾏｽﾀｰ鍵

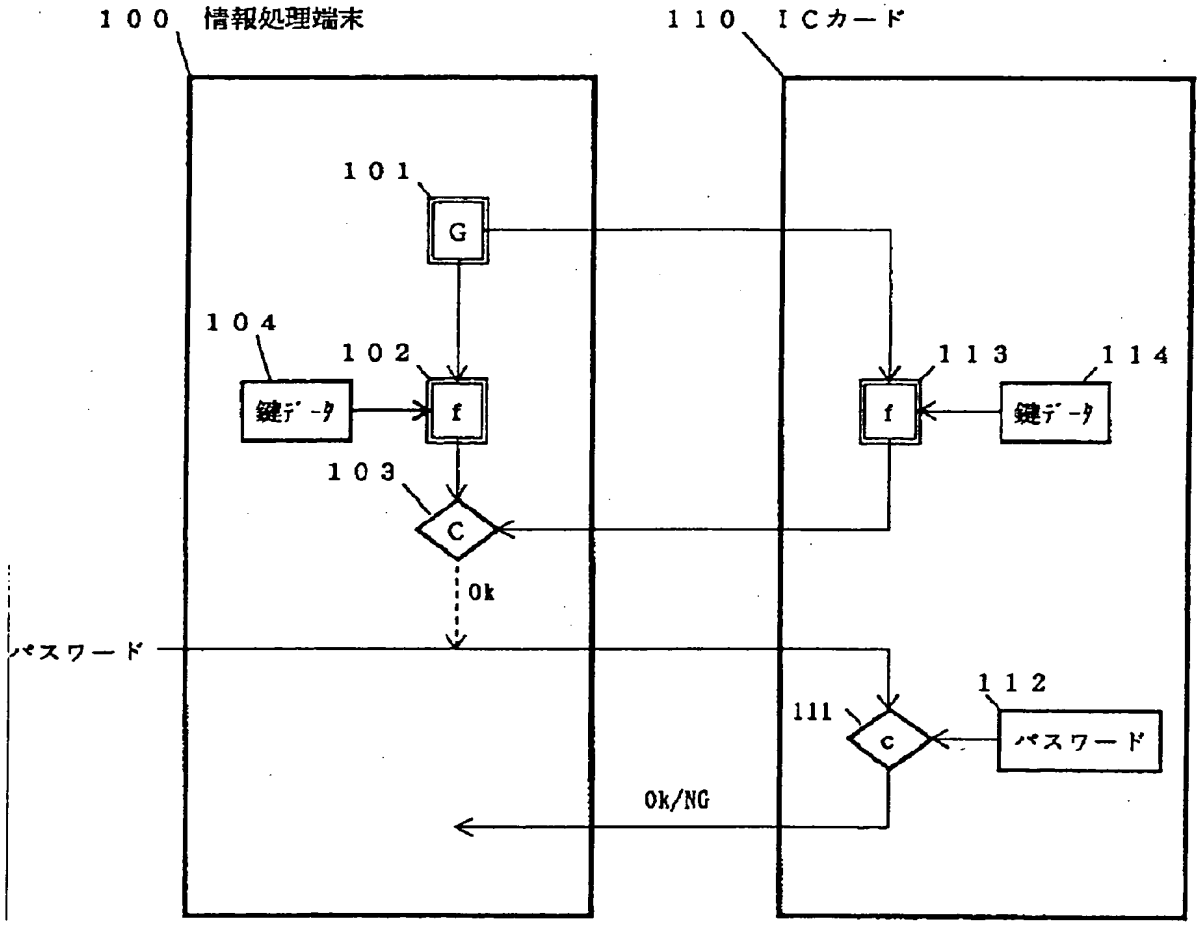
【図２】


２０　小売店端末
４０　ユーザカード
２１
識別子
30 小売店ｶｰﾄﾞ
４３
４２
４５
G
F
ﾏｽﾀｰ鍵
３２
３１
４１
認証鍵
f
f
認証鍵
４４
Ok
C

【図３】


２０　小売店端末
２１
識別子
３０　小売店ｶｰﾄﾞ
３２
３１
認証鍵
ｆ
５０
Ｈ
ｾｯｼｮﾝ鍵
５１
Ｄ
データ
４０　ユーザカード
４３
４２
４５
Ｇ
Ｆ
ﾏｽﾀｰ鍵
４１
ｆ
認証鍵
５２
Ｈ
４４
Ｃ
Ok
ｾｯｼｮﾝ鍵
５３
５４
Ｅ
データ

【図４】



フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
		8623-5L	G06K 19/00	P
		8949-5K	H04L 9/00	Z